Armis Centrix™ for for VIPR – Prioritization and Remediation | for Healthcare

More Assets, More Cyber Exposure

The healthcare industry is one of the most targeted by advanced cyberattacks, with widespread threats from ransomware, unpatched vulnerabilities, third-party risks, and data breaches. Increased reliance on innovation and digital patient care translates to more assets, devices, and interconnections between them. The technology landscape has dramatically expanded, bringing with it an influx of cyber exposure risk, alerts, and vulnerabilities. Without a clear prioritization and remediation strategy, the volume of alerts and security findings can overwhelm already underresourced teams, creating massive security gaps that can compromise patient safety and the continuity of care.

From imaging systems and wearable monitors to supporting IT infrastructure, security teams at healthcare delivery institutions are tasked with managing a wide attack surface. To minimize the risk of exploits, impacts on care availability and patient outcomes, all vulnerabilities, as well as risk factors such as end-of-life (EOL) assets, must be viewed through both a cyber exposure management and clinical lens for effective prioritization and remediation.

Patient-Centric Vulnerability Management

A patient-centric approach to vulnerability management must prioritize the biggest risks to patient safety, care delivery, and operational continuity to prevent downtime and potential harm. With Armis Centrix™ for VIPR – Prioritization and Remediation, you can drastically reduce the effort involved in vulnerability management and address the biggest potential interferences in clinical care by eliminating the time it takes to sort through alerts manually and targeting a prioritized list of the biggest risks that matter most to your organization.

Collect, deduplicate, contextualize, and prioritize these findings into actionable fixes based on their clinical and operational risk profile. Automatically assign owners and initiate remediation workflows, prioritized based on asset criticality and clinical risk score. This allows the organization to focus efforts on addressing the biggest impacts on patient safety, data confidentiality, and potential care disruptions. Avoid unnecessary delays in care or downtime of medical devices due to unaddressed security incidents and lengthy and complex mitigation processes.

Critical VIPR – Prioritization and Remediation Use Cases

Discover and Consolidate

Automatically consolidate and view an aggregated list of all risks from different sources for every asset, including IT, OT, medical, and IoT devices.

Contextualize

Assign clinical context to findings, including likelihood of exploit, threat intelligence, and asset attributes, including location, proximity to patient care, utilization, medical device recalls, and clinical risk score.

Prioritize

Automate prioritization based on the real risk to your organization, threat severity, and patient care impact. Focus on high-impact fixes that will resolve the largest number of security issues and patient safety risks.

Assign and Remediate

Leverage predictive capabilities to determine who is most likely responsible for the asset to eliminate guesswork and streamline remediation.

Monitor and Report

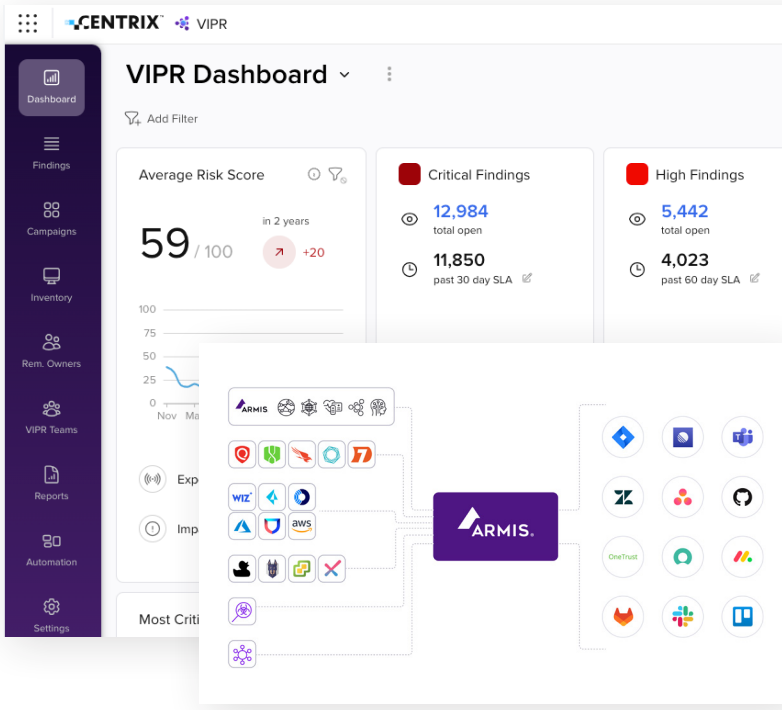
Track, monitor, and demonstrate progress for both individual remediation tasks and overall security posture, risk activity, and trends in the organization over time

Key Features that make Armis Centrix™ the go-to platform for Vulnerability Prioritization and Remediation

- **Streamlined risk assessment and remediation** - with automatic consolidation, deduplication, contextualization, and prioritization based on asset profile and clinical context.
- **Automated prioritization** - Clearly determine remediation priorities based on evaluation of environmental factors and asset criticality to maximize efforts.
- **Integrated asset inventory and enrichment** - for the most comprehensive risk and asset information to inform actions.
- **Customized asset labels and configurable risk scoring** - Focus on the risks most important to your environment.
- **Predictive ownership assignment** - Leverage AI to assign asset owners to connect security findings to the fix, speeding up time to remediation and eliminating manual effort and guesswork.
- **Centralized remediation monitoring** - For a comprehensive view of all security findings and alerts, and drill-down capabilities across every asset.
- **Bidirectional ticketing and workflow integrations** - Initiate remediation efforts and track to completion for effective collaboration.
- **Risk Simulator** - Assess potential risk reductions of an action on your overall security posture to take actions on the biggest potential improvements.
- **Dashboards and reporting** - To demonstrate targeted risk reduction and ongoing security posture across the organization.

Why more businesses are trusting Armis to drive measurable outcomes

1. **Impactful Actions**
   Translates millions of alerts to thousands of grouped findings
2. **Efficiency**
   75% improved MTTR for the right findings to reduce risk
3. **Maximize Efforts**
   Streamline time spent on manual assessment of alerts and prioritization by 80%
4. **Operational Resilience**
   Reduce operational overhead by 90% with targeted remediation efforts, AI-powered asset ownership assignment, and asset intelligence
5. **Focus**
   Halve the time for resolution of critical findings and scale remediation with bulk ticketing for findings with a common fix



Next-gen Approach to Close the Gap Between Finding and Fixing Risk

Visit **Armis.com** to find out more